"Express Mail" mailing label number: EL737389092US
Date of Deposit: 10/11/01
I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" services under 37 C.F.R. 1.10 on the date indicated above and is addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231.
Typed Name of Person Mailing Paper or Fee: Dianna Baker
Signature: D Baker

PATENT APPLICATION
DOCKET NO. 10007585-1

DEVICE CONFIGURATION METHOD AND APPARATUS

INVENTORS:
Robert E. Haines

DEVICE CONFIGURATION METHOD AND APPARATUS

COPYRIGHT NOTICE

FIELD OF THE INVENTION

The invention relates to printers and other hard copy output engines. More particularly, the invention relates to hard copy output engine consumable supply management and related methods.

BACKGROUND OF THE INVENTION

As computer systems and data communications systems have developed, the number and variety of hard copy output engines employed in a typical office or factory setting has grown. Examples include photo copiers, facsimile machines, printers and devices including more than one of these capabilities. In turn, this has led to a need to be able to order greater number of consumable supplies, some of which are specific to specific types of hard copy output engines.

As need for these types of hard copy output engines has grown, a number of different manufacturers have developed different hard copy output engines providing different operational characteristics and capabilities. While some consumable commodities associated with these devices are common to most or all such devices (e.g., standardized paper sizes), other consumable commodities, such as toners and toner supply cartridges or ink reservoirs, tend to be unique to a specific manufacturer. Additionally, different hard copy output engines may have different paper capacities, capabilities for accepting more or fewer paper sizes and different toner or other pigment supply requirements and capacities.

It is generally helpful to have a mechanism for keeping track of usage of consumable commodities in keeping computer systems functional, and to determine when periodic or aperiodic maintenance is desirable. For example, it is extremely

helpful to ensure that adequate supplies of replacement print media and pigmentation or marking material are available when needed.

Coordination of orders for supplies can be very helpful to avoid over- or under-stocking of these consumable commodities, while still achieving the benefits of economies of scale by pooling orders to service multiple hard copy output engines, especially those using at least some of the same consumable commodities. However, in many business settings, the sheer number of diverse hard copy output engines being used in different aspects or divisions of the business may lead to confusion in maintaining adequate supplies of these consumable commodities.

What is needed is a way to facilitate provision of data providing a communications link to suppliers of consumable commodities, as well as data describing consumable commodity status, for a network including one or more hard copy output engines.

SUMMARY OF THE INVENTION

In accordance with an aspect of the present invention, a method of configuring a hard copy output engine includes downloading data including a configuration plug-in and configuration data each including user-specified information and configuring the hard copy output engine using the downloaded data.

In accordance with another aspect of the present invention, an article of manufacture comprising a computer usable medium has computer readable code embodied therein. The computer readable code is configured to cause a processor to download data including a configuration plug-in and configuration data each including user-specified information and configure a hard copy output engine using the downloaded data.

In accordance with yet another aspect of the present invention, a computer implemented control system for a hard copy output engine includes memory configured to store a software module and processing circuitry configured to employ the software module. The processing circuitry is configured to employ the software module to download data including a configuration plug-in and configuration data each including user-specified information and to configure a hard copy output engine using the downloaded data.

Other features and advantages of the invention will become apparent to those of ordinary skill in the art upon review of the following detailed description, claims and drawings.

DESCRIPTION OF THE DRAWINGS

Fig. 1 is a simplified block diagram of a computer network including a computer, a hard copy output engine and a firewall, in accordance with an embodiment of the present invention.

Fig. 2 is a simplified flow chart of a process P1 illustrating how a system can interact with a vendor website across the firewall of Fig. 1 to enable a peripheral device, such as the hard copy output engine, to exchange information with a vendor website via an embedded web server, in accordance with an embodiment of the present invention.

Fig. 3 is a flow chart illustrating steps in carrying out a process P2 for configuring devices discovered in the process P1 of Fig. 2, in accordance with an embodiment of the present invention.

Fig. 4 is a flow chart illustrating steps in carrying out a process P3 for setting preferences for resellers and for identifying purchasers for consumables and service for devices discovered in the process P1 of Fig. 2, in accordance with an embodiment of the present invention.

Fig. 5 is a simplified flow chart of a process P4 for setting inventory parameters for the group or groups of peripheral devices identified in the process P1 of Fig. 2, in accordance with an embodiment of the present invention.

Fig. 6 is a simplified flowchart of a process P5 for configuring a peripheral device, such as a hard copy output engine, using information collected via the processes of Figs. 2 through 5, in accordance with an embodiment of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

Fig. 1 is a simplified block diagram of a computer network 10 including a computer 12 and a hard copy output engine 14, in accordance with an embodiment of the present invention. The computer 12 is coupled to the hard copy output engine 14 via a bus 16 allowing either the computer 12 or the hard copy output engine 14 to initiate data communications with the other. In one embodiment, the hard copy output

engine 14 is a device such as a printer, copier, facsimile machine or a multifunction device capable of providing two or more such functions. It will be appreciated that while Fig. 1 illustrates only a single computer 12 and a single peripheral device 14 for ease of illustration and convenience in understanding, multiple computers 12 and peripheral devices 14 may all be coupled to the bus 16.

In one embodiment, the system 10 is coupled to an external interconnection 17 via a data path 18. In one embodiment, the data path 18 includes an intranet. In one embodiment, the data path 18 includes a local area network (LAN) or wide area network (WAN). In one embodiment, the data path 18 includes access to the Internet via a firewall 19.

Security is a constant challenge for networks and computing engineers responsible for networks, and is discussed in commonly-assigned U.S. Patent No. 6,192,410 B1, entitled "Methods And Structures For Robust, Reliable file Exchange Between Secured Systems", issued to Miller et al. and which is hereby incorporated herein by reference. In particular, and as discussed in the afore-noted patent, it is important in wide area network applications for computing systems attached to such a network to secure their resources from inappropriate, unauthorized access. The Internet is an example of a global wide area network where security measures are often critical to an ongoing business enterprise connected to the Internet. Such security measures are required to assure that unauthorized third parties, anywhere in the world, cannot gain access to sensitive materials within the enterprise via the global, publicly accessible, Internet.

Though such security measures or firewalls 19 are vital to secure each particular enterprise, their very existence creates the burden for those trying to legitimately exchange information between enterprises via such global, public networks. A user in one particular computing enterprise encounters a number of difficulties exchanging data with another user in a different computing enterprise via computer system to computer system network communication links. Though the communication capability may exist, for example via the Internet, safeguards and security measures (firewalls 19) within each enterprise makes such enterprise-to-enterprise exchanges difficult - exactly as they are intended to do.

In general, such firewall 19 security measures operate at lower layers of the network communication layered model to filter out potentially harmful network data

exchange. For example, the firewall 19 may permit certain protocols to be exchanged only among certain network devices known to be physically secured within the enterprise. Network devices not within the permitted scope of secured devices are not permitted to use the filtered protocols. Should such un-authorized devices attempt such communications, the firewall 19 simply discards their network data transfer requests. As a result, a vendor may not be able to initiate data communications between a database maintained by the vendor and devices that have been deployed at clients of that vendor or allied vendors.

In one embodiment, the computer 12 and the hard copy output engine 14 are capable of exchanging data via a protocol compatible with presence of other computers 12 or hard copy output engines 14 on the bus 16. In one embodiment, the computer 12 and the hard copy output engine 14 employ an object-oriented request-reply protocol supporting asynchronous printer query, control and monitor capabilities, and that is capable of documenting the requests, replies and data types supported by the protocol. In one embodiment, a protocol known as PML is used.

The term "PML" refers to Printer Management Language, which has been developed by the Hewlett-Packard Company of Palo Alto, California. Further description of PML can be found at http://www.hp.com or at http://www.hpdevelopersolutions.com, by entering a user name, a user selected password, and by joining a solutions provider program. More particularly, a PML Protocol Specification, Hewlett-Packard Company, 11/18/98, Revision 2.3 is available therein, and is hereby incorporated herein by reference.

One exemplary remote query language implemented within the network system is a Simple Network Management Protocol (SNMP). In such an exemplary configuration, host devices such as personal computers 12 include respective processing circuitry (not shown) operable to formulate an appropriate SNMP query or request which is addressed to one or more appropriate computer peripheral devices using a communication medium. The appropriate computer peripheral device(s) receive the query or request and provide information back to appropriate host devices or computers 12 using the communication medium. Protocols other than SNMP are utilized in other embodiments to implement communications within the system.

PML permits many applications to exchange device management information with numerous computer peripheral devices, such as image forming

devices. Individual computer peripheral devices implement any conversion operations between the protocol used to exchange information with respect to computer peripheral devices (e.g., SNMP) and the internal protocol (e.g., PML) used within the respective computer peripheral devices.

In one embodiment, the data path 18 provides common gateway interface (CGI) data communication capability. In one embodiment, the data path 18 includes an email capability (e.g., simple mail transfer protocol or SMTP) for facilitating data communication. In one embodiment, the data path 18 includes a secure data path using HTTP (hyper text transfer protocol) with SSL (secure sockets layer), as is described in more detail in U.S. Patent No. 5,657,390, entitled "Secure Socket Layer Application Program Apparatus And Method", issued to Elgamal et al. and U.S. Patent No. 6,081,900, entitled "Secure Intranet Access", issued to Subramanian et al., which patents are hereby incorporated herein by reference for their teachings.

The hard copy output engine 14 includes a controller 20, such as a conventional microprocessor or microcontroller. The hard copy output engine 14 also includes one or more sensors 22 coupled to the controller 20 and a memory 24 in data communication with the controller 20. In one embodiment, the memory 24 comprises conventional volatile and non-volatile memory units. In one embodiment, the memory 24 includes magnetic, magneto-optic or optical storage media, such as conventional disc storage or floppy disc data storage units, or memory integrated circuits, CD-ROMs or the like. In one embodiment, the hard copy output engine 14 accepts instructions as a computer instruction signal embodied in a carrier wave carrying instructions executable by the controller 20.

The sensors 22 are coupled to consumable commodities associated with the hard copy output engine 14. In one embodiment, when the sensors 22 report that a quantity of a consumable commodity (e.g., print media, paper, toner or ink) associated with the hard copy output engine 14 has decreased to below a predetermined threshold amount, or that malfunction of a dispenser of a consumable commodity exists, the controller 20 initiates a data communication ultimately intended for transmission via the data path 18. Additionally, the sensors 22 may track data such as number of sheets of media that have been printed, in order to schedule maintenance operations.

The controller 20 and the memory 24 also comprise an embedded web server 26. Embedded web server 26 refers to a web server that is completely contained within a device, such as a computer peripheral device. Embedded web servers 26 are configured to provide management information about the peripheral device. An embedded web server 26 can be used to manage or manipulate individual peripheral devices, such as the hard copy output engine 14, that are present in the network 10. A web browser can be used by a network user to access an embedded web server 26 in order to obtain device status updates, perform troubleshooting operations, change device configuration settings and to link to online customer support.

The term "web browser" refers to an application that runs on a workstation or personal computer 12 within the network environment 10, that lets users view HTML documents via the Internet, to access hyperlinks and to transfer files. In operation, web browsers request information from web servers and display the information that the web servers send back. The information is organized into pages containing text, graphics, sound and animation formatted by HTML and Java® applets.

The term "web server" refers to a specialized program running on a server that supports TCP/IP protocol. Web servers enable workstations or personal computers 12 or other devices in the network 10 to access external networks such as the Internet. Web servers receive HTTP requests that browsers running on various types of computer systems send. The web server could be asked to get a text or graphics file, retrieve a ZIP file or run a program. The web server then sends the information, files or program results back to the requesting browser. Embedded web servers 26 are contained within the hard copy output engine 14 itself to provide management information about the hard copy output engine 14.

Fig. 2 is a simplified flow chart of a process P1 illustrating how a system can interact with a vendor website across the firewall 19 of Fig. 1 to enable a peripheral device, such as the hard copy output engine 14, to exchange information with the vendor website via the embedded web server 26, in accordance with an embodiment of the present invention.

Initially, it is desirable to provide the vendor site with a list of system components, such as peripheral devices, associated with that vendor. This process

is called "device discovery". Device discovery needs to take place at least once for each device that is to be supported via the vendor website. The vendor website is a website associated with the peripheral device. In one embodiment, the vendor website may be a website for an OEM that manufactured the peripheral device. In one embodiment, the vendor website may be a website for a remanufacturer that remanufactures or reconditions consumables, such as pigmentation or marking material (e.g., toner or ink cartridges), for the peripheral device. In one embodiment, the vendor website may be a website for a vendor of peripheral devices that compete with the manufacturer that produced the peripheral device.

The process P1 is initiated when the MIS manager browses the vendor website in a step S11.

In a step S12, the MIS manager downloads a device discovery plug in via the web browser contained in the MIS manager's computer 12.

In a step S13, the device discovery plug in engages in device discovery, that is, inventories peripheral devices that are coupled to the bus 16 that are also associated with that vendor. In one embodiment, the device discovery plug in includes information entered by the MIS manager regarding peripheral devices that the MIS manager knows have been added to the system or that have been modified.

In one embodiment, the device discovery plug in acts as a proxy for the vendor web site within the network 10 to poll and identify peripheral devices and their addresses in the network 10 that are associated with that vendor. In one embodiment, peripheral devices are identified via serial numbers. In one embodiment, the device discovery plug in determines make and model number, as well as options, for each peripheral device associated with that vendor.

In a step S14, the discovered device information is stored for reference. In one embodiment, the device information is stored in memory associated with the vendor website.

In a step S15, the device information is sorted into suitable groups. For example, peripheral devices may be grouped according to internal business structures associated with the network 10, e.g., research and development, accounting etc. that may also correspond to specific areas within a facility.

In a step S16, group names are stored for reference. In one embodiment, the group names and data relevant to the individual devices are stored in a memory associated with the vendor web site.

In a step S17, a purchase authorizer is identified for each of the groups determined in the step S15. The purchase authorizer is responsible for authorizing purchases of consumables associated with the peripheral devices and for authorizing periodic and aperiodic maintenance. Additionally, the vendor may provide information to the purchase authorizer regarding product upgrades or accessories as these become available.

In a step S18, maintainers are identified for the groups identified in the step S15. In one embodiment, email addresses for maintainers are collated with the groups identified in the step S16. In one embodiment, the email addresses are stored with the groups in a memory associated with the vendor web site.

The process P1 then ends. The process P1 provides a way for a vendor website to obtain information from a private network 10 across the firewall 19 without compromise of the security of the private network 10. The process P1 also does not require any added hardware for the network 10.

Fig. 3 is a flow chart illustrating steps in carrying out a process P2 for configuring the devices that were discovered in the process P1 of Fig. 2, in accordance with an embodiment of the present invention. The process P2 begins in a step S21.

Optionally, the process P2 may be initiated by the vendor web site sending an email to the maintainer in the step S21 using the email address obtained in the step S18 of the process P1 of Fig. 2. The email may include information specific to the group of devices identified as being associated with that maintainer in the step S18 of the process P1.

Alternatively, the process P2 may be initiated by the maintainer of the peripheral devices. In either case, the maintainer launches a web browser to interact with the vendor web site in a step S22. In one embodiment, the maintainer launches the web browser using a URL contained in the email message received by the maintainer in the step S21. In one embodiment, the URL is specific to the list of peripheral devices associated with the maintainer.

In a step S23, the maintainer browses the vendor web site to configure a portion of the vendor web site. In one embodiment, the maintainer sets maintenance notification thresholds. For example, some types of maintenance may be set to take place after a predetermined number of sheets of media have been printed, or following a predetermined number of hours of operation, or may be based on other operation-dependent or seasonal criteria.

In a step S24, the maintainer sets thresholds for replenishment of consumables. In one embodiment, these are set via interaction with the vendor web site.

In a step S25, the vendor web site collates the thresholds set by the maintainer and sends back an electronic message including configuration data to be used by the embedded web server 26 in the peripheral device. In one embodiment, an email including a hotlink having an attached CGI script or an XML list is sent from the vendor web site to the maintainer. A hotlink is an Internet address, usually in the form of a URL (universal resource locator) that can be readily activated, for example by selecting it with a mouse or other tactile input device, to access the web site at that Internet address.

In a step S26, the maintainer then uses this electronic communication to set the thresholds in the peripheral device via the embedded web server 26.

In one embodiment, the vendor web site provides a hot link at the vendor web site that, when activated by the maintainer, performs substantially the equivalent of the steps S25 and S26.

In one embodiment, the vendor web site may send an email directly to the embedded web server with the configuration data in the step S25. The embedded web server 26 then uses this electronic communication to set the thresholds in the peripheral device via the embedded web server in the step S26. In one embodiment, the email may be sent to a system administrator to be forwarded to the peripheral device. This allows additional screening to address potential security concerns.

In one embodiment, a device configuration plug in becomes part of the browser. The plug in takes the configuration data from the vendor web site and configures the peripheral. In one embodiment, SNMP is used to configure PML objects to configure the peripheral.

For example, the maintainer may need to be aware of an upcoming shortfall of media or pigmentation or marking material and thus may want to have the re-ordering process start when the supply falls to a predetermined level. Alternatively, the maintainer may prefer to have the re-ordering process initiate when the consumable is essentially depleted. Additionally, the maintainer may want to pool consumable orders over a group of peripherals or over time. The maintainer may also want to coordinate maintenance of local stocks of consumables with changes in consumption, and may opt to replace some consumables that would not otherwise be replaced when other consumables require replacement (e.g., replace a low toner cartridge of one color when another toner cartridge is exhausted) in order to optimize labor content.

The process P2 then ends.

Fig. 4 is a flow chart illustrating steps in carrying out a process P3 for setting preferences for resellers and for identifying purchasers for consumables and service for the devices that were discovered in the process P1 of Fig. 2, in accordance with an embodiment of the present invention. The process P3 begins in a step S31.

Optionally, the process P3 may be initiated by the vendor web site sending an email to the purchase authorizer in the step S31 using the email address obtained in the step S17 of the process P1. The email may include information specific to the group of devices identified as being associated with that purchase authorizer and maintainer in the step S18 of the process P1.

Alternatively, the process P3 may be initiated by the purchase authorizer for consumables for the peripheral devices. In either case, the purchase authorizer launches a web browser to interact with the vendor web site in a step S32. In one embodiment, the purchase authorizer launches the web browser using a URL contained in the email message received by the maintainer in the step S31. In one embodiment, the URL is specific to the list of peripheral devices associated with the purchase authorizer.

In a step S33, the purchase authorizer identifies purchasers associated with the group of peripheral devices identified in the process P1. In one embodiment, the purchase authorizer provides email addresses for the purchasers, and these may be stored in a memory associated with the vendor web site.

In a step S34, the purchase authorizer identifies preferred resellers of consumables for the peripheral devices, and these may be stored in a memory associated with the vendor web site.

The process P3 then ends.

Fig. 5 is a simplified flow chart of a process P4 for setting inventory parameters for the group or groups of peripheral devices identified in the steps S15 and S16 of the process P1 of Fig. 2, in accordance with an embodiment of the present invention. The process P4 begins in a step S41.

Optionally, the process P4 may be initiated by the vendor web site sending an email to the purchaser in the step S41 using the email address obtained in the step S17 of the process P1. The email may include information specific to the group of devices identified as being associated with that maintainer in the step S33 of the process P3.

Alternatively, the process P4 may be initiated by the purchaser for consumables for the peripheral devices. In either case, the purchaser launches a web browser to interact with the vendor web site in a step S42. In one embodiment, the purchaser launches the web browser using a URL contained in the email message received by the purchaser in the step S41. In one embodiment, the URL is specific to the list of peripheral devices associated with the purchaser.

In a step S43, the purchaser may set group order threshold settings, and these may be stored in a memory associated with the vendor web site. This may be used to combine orders to service needs for a group of peripheral devices using a local store of consumables as a buffer.

In a step S44, the purchaser may set current inventory levels for the local store of consumables, and these may be stored in a memory associated with the vendor web site.

In a step S45, the purchaser sets minimum inventory order trigger thresholds, and these may be stored in a memory associated with the vendor web site.

In a step S46, the purchaser sets maximum target inventory levels, and these may be stored in a memory associated with the vendor web site.

In a step S47, the purchaser sets order notification settings, and these may be stored in a memory associated with the vendor web site.

The process P4 then ends.

Fig. 6 is a simplified flowchart of a process P5 for configuring a peripheral device, such as a hard copy output engine, using the information collected via the processes P1 through P4 of Figs. 2 through 5, in accordance with an embodiment of the present invention.

In one embodiment, the data collected by the processes P1 through P4 are used to derive XML configuration data in a step S51.

These data are then emailed from the vendor web site to the network 10 in a step S52. In one embodiment, the data are emailed directly to the embedded web server 26 of the hard copy output engine 14 or other peripheral device in the step S52. In one embodiment, the data include a hotlink configured to activate a browser and direct it to the vendor website.

In one embodiment, the data are emailed to a responsible party for review in the step S52. In this embodiment, the data are forwarded, for example via email, to the embedded web server 26 after review by the responsible party in an optional step S53.

In a step S54, the XML configuration data interact with the embedded web server 26 to set thresholds in the peripheral device, such as the hard copy output engine 14. In one embodiment, the responsible party activates a browser using the hotlink and uses the browser to configure the peripheral device.

In one embodiment, the data collected by the processes P1 through P4 are used to derive XML configuration data that are then emailed to the network 10 in the step S52. In one embodiment, a CGI script is used to convey the configuration data.

The process P5 then ends.

While the flowcharts of Figs. 2 through 6 assume that separate individuals fill the roles of MIS manager, maintainer, purchase authorizer and purchaser, it will be appreciated that some or all of these roles may be played by one or more persons, or by more or fewer persons. It will also be appreciated that many of the acts of Figs. 2 through 6 need not occur in the order in which they are described and may take place contemporaneously.

Benefits include allowing the user to configure the hard copy output engine for ease of ordering and maintaining supplies of consumables. This is accomplished

without requiring the user to add software modules or hardware to the network 10. Additionally, the firewall 19 maintains integrity of the system 10.

The protection sought is not to be limited to the disclosed embodiments, which are given by way of example only, but instead is to be limited only by the scope of the appended claims.